On The Achievable Rate Region of a New Wiretap Channel With Side Information

† Hamid G. Bafghi, †Babak Seyfe, ‡Mahtab Mirmohseni,‡M. Reza Aref

† Electrical Engineering Department, Shahed University, Tehran, Iran.

†‡ ISSL Laboratory, Electrical Engineering Department, Sharif University of Technology, Tehran, Iran.

Emails: {ghanizade, seyfe}@shahed.ac.ir, mirmohseni@ee.sharif.edu, aref@sharif.edu

Abstract

A new applicable wiretap channel with separated side information is considered here which consist of a sender, a legitimate receiver and a wiretapper. In the considered scenario, the links from the transmitter to the legitimate receiver and the eavesdropper experience different conditions or channel states. So, the legitimate receiver and the wiretapper listen to the transmitted signal through the channels with different channel states which may have some correlation to each other. It is assumed that the transmitter knows the state of the main channel non-causally and uses this knowledge to encode its message. The state of the wiretap channel is not known anywhere. An achievable equivocation rate region is derived for this model and is compared to the existing works. In some special cases, the results are extended to the Gaussian wiretap channel.

Index Terms

Equivocation rate, secrecy capacity, side information, wiretap channel, perfect secrecy.

I. Introduction

Secure communication from an information theoretic perspective was first studied by Shannon in his famous paper [1], where a noiseless channel model was assumed with an eavesdropper which has an identical copy of the encrypted message as a legitimate receiver, and the sufficient and necessary condition for perfect secrecy using

information theoretic concepts were established. In the Shannon's model, a source message W is encrypted to a ciphertext E by a key K shared by the transmitter and the receiver. An eavesdropper, which knows the family of encryption functions, i.e., keys and the probability of choosing the keys, may intercept the ciphertext E. The system is considered to be perfectly secure if the a posteriori probabilities of W for all E would be equal to the a priori probabilities, i.e., $P(W|E) = P(W)$. Alternatively, Shannon proved that the perfect secrecy can be achieved only when the secret key is at least as long as the plaintext message or more precisely, when $H(K) \geq H(W)$.

The wiretap channel was first introduced and studied by Wyner in his fundamental paper [2] which is the most basic physical layer model explains the communication security's problems. In his model, the transmitter wishes to transmit a source signal, i.e., a confidential message, to a legitimate receiver in a way that this message be kept secret from an eavesdropper. In this model illustrated in Fig. 1, despite of the Shannon's model, it is assumed that the channel to the eavesdropper is a physically degraded version of the channel to the legitimate receiver. In other words, the channel's output at the eavesdropper may be a noisy version of the channel output at the legitimate receiver. On the other hand, the transmitter communicates to the intended receiver through the main channel which may be noisy or noiseless, but the wiretapper receives a noisy copy of the message through a wiretap channel which is a cascade of the main channel. In addition, Wyner [2] assumed that the eavesdropper knows the transmitter's encoding-decoding scheme. So, the objective is maximizing the rate of reliable communication such that the wiretapper realizes as little as possible about the source output. The information leakage was measured by equivocation rate as $\Delta \triangleq H(S^K|Z^N)$, where S^K and Z^N are represented the message set and the channel output at the wiretapper, respectively. Eavesdropper is assumed to be a passive receiver which does not transmit any signal over the channel. Furthermore, Wyner [2] proposed a basic principle coding strategy to achieve secure communication for wiretap channels which is based on the fact that the eavesdropper is not able to decode any information more than it's channel capacity.

Csiszár and Körner generalized the Wyner's wiretap channel [3]. In their model, it is assumed that the wiretap channel's output is not necessarily a degraded version of the legitimate receiver's one. They showed that the secrecy capacity can be expressed as $C_s = max_{U \to X \to (Y,Z)}[I(U;Y) - I(U;Z)]$, where X, Y and Z are the channel input, the channel output in the legitimate receiver and the channel output at the wiretapper, respectively. Moreover, the

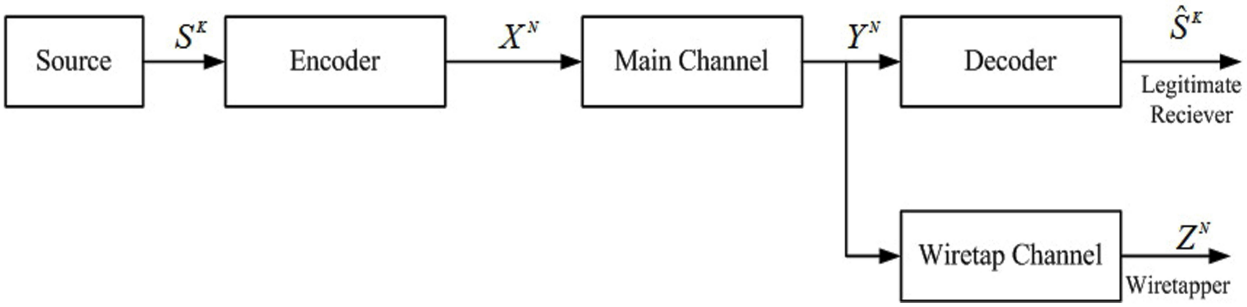

Fig. 1. Wyner's Wiretap channel [2]. In this channel, it is assumed that the channel to the eavesdropper is physically degraded version of the channel to the legitimate receiver.

maximization is over all random variables U in joint distribution with X, Y and Z such that $U \to X \to (Y, Z)$ forms a Markov Chain.

Using the channel state information in communication channel models was introduced by Shannon in his landmark paper [4], where he assumed the availability of Channel Side Information at the Transmitter (CSIT). Gel'fand and Pinsker in their essential work [5] proved that the capacity of the state-dependent discrete memoryless channel with non-causally CSIT is given by $C = max_{p(u,x|v)}[I(U;Y) - I(U;V)]$, where the maximum is taken over all input distribution $p(u, x|v)$ with a finite alphabet auxiliary random variable U.

Costa in his well known paper named *Writing on Dirty Paper*, extended this result to the Gaussian channel and showed that for this channel, interference did not affect the capacity [6]. He chose $U = X + \alpha V$ and maximized the Gel'fand and Pinsker's capacity over all quantity of α and proved that for this value of α, the capacity of the channel reduces to the channel without states. The dirty paper channel was extended to the basic Gaussian wiretap channel with side information by Mitrpant and et al. [7], in which an achievable and upper bound for this channel has been introduced.

Chen and Vinck investigated Wyner's wiretap channel with side information [8] (Fig. 2). Their results are based on the previous wiretap channel's results in [2], [3], [7] and the discrete memoryless channel with state information [5]. They gave an achievable rate region which is established using a combination of the Gel'fand-Pinsker coding and the Wyner's wiretap coding. They extended their results to the Gaussian wiretap channel with side information

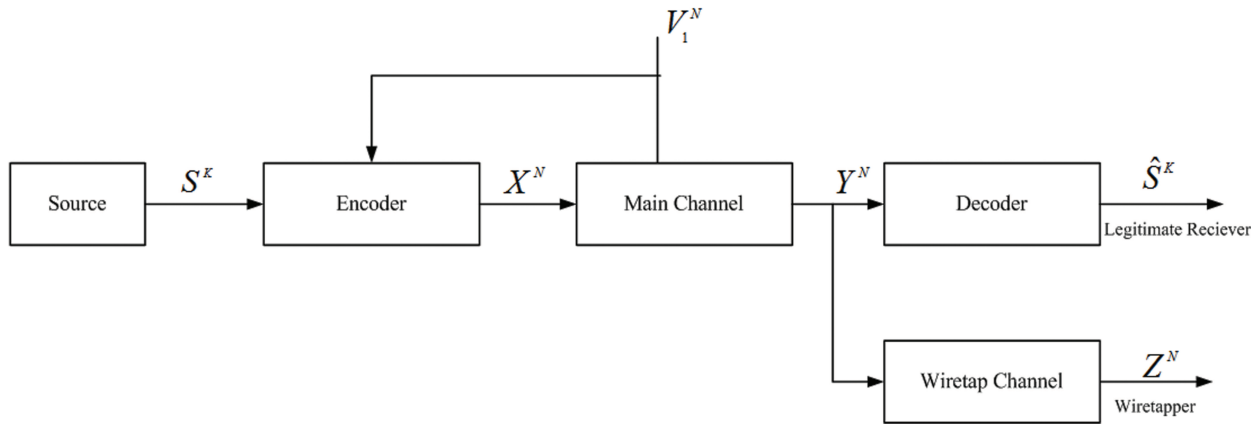

Fig. 2. Wiretap channel with side information introduced by Chen and Vinck [8].

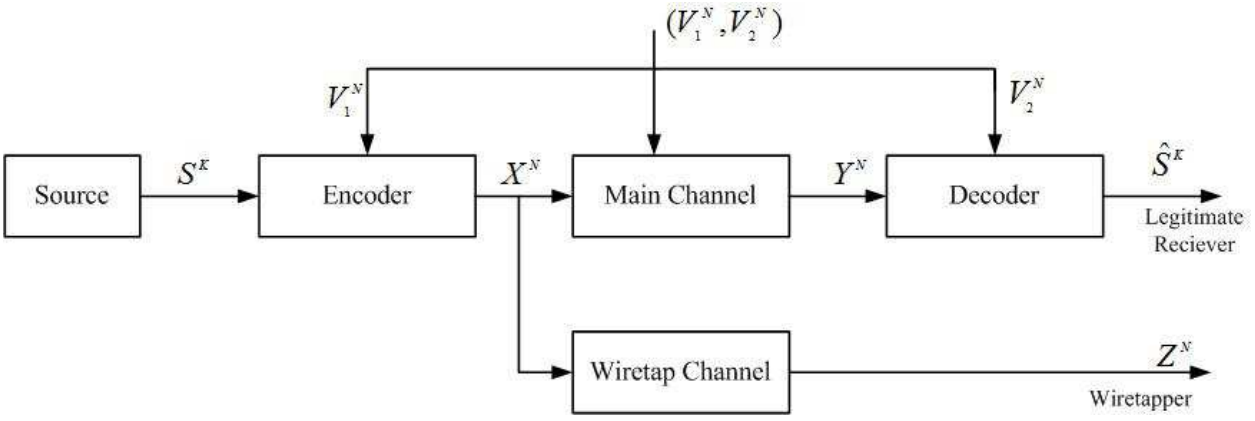

Fig. 3. Wiretap channel with two–sided channel state information [9].

using the same technique like dirty paper channel [8].

Furthermore, there were some different works on the wiretap channel with and without side information. The work [10] studied the two way wiretap channel. The Gaussian wiretap channel with m-pam inputs was considered in [11] and the secrecy capacity of the Gaussian MIMO multi-receiver wiretap channel was investigated by [12]. Liu et al. in [9], studied the two-sided channel state problem in the discrete memoryless wiretap channel, where as shown in Fig. 3, the information of the two-sided channel states are available at the transmitter and the main receiver, respectively. In addition, in their scenario the wiretap channel is not necessarily a degraded version of the main channel. An achievable rate equivocation region for this general case is given in [9]. Khisti et. al., considered

the secret-key agreement problem in the wiretap channel [13], [14]. In their model, the transmitter communicates to the legitimate receiver and the eavesdropper over a discrete memoryless wiretap channel with a memoryless state sequence. The transmitter and the legitimate receiver generate a shared secret key that remains secret from the eavesdropper. The results are comparable to the wiretap channel introduced by [8]. Recently, an improved lower bound for the wiretap channel with causal state information at the transmitter and receiver has been reported in [15], where the achievability of the rate region is proved using block Markov coding, Shannon strategy, and key generation from the common state information [4]. The state sequence available at the end of each block, is used to generate a key which is used to enhance the transmission rate of the confidential message in the following block.

In this paper, we introduce a new wiretap channel model with side information, in which the wiretapper's messages is not a degraded version of the legitimate receiver's one. On the other hand, the transmitter sends its message through the main and the wiretap channels. So, the receiver and the wiretapper listen to the sent message from the separated channels with different characteristics, i.e., different channel states. This model is a general case of Chen–Vinck [8] and Wyner wiretap channel [2] and reduces to these channels in special cases. We extend our model to the Gaussian wiretap channel where the states of the main and wiretapper channels are different with some correlation coefficients. In the Gaussian case, if the correlation coefficients are equal to one, our channel reduces to Chen–Vinck's channel. The proposed channel is illustrated in Fig. 4. The rest of the paper is organized as follows. In Section II, the channel model is introduced. The main results are presented in Section III. In Section IV, the proof of the main results are given. In Section V, the results are extended to the Gaussian case and the paper is concluded in the last section.

II. Channel Model and Preliminaries

First, we clear our notation in this paper. Let $\mathcal{X}$ be a finite set. Denote its cardinality by $|\mathcal{X}|$. If we consider $\mathcal{X}^N$, the members of $\mathcal{X}^N$ will be written as $x^N = (x_1, x_2, ..., x_N)$, where subscripted letters denote the components and superscripted letters denote the vector. A similar convention applies to random vectors and random variables, which are denoted by uppercase letters.

Consider the situation shown in Fig. 4. Assume that the state information of the main channel, i.e., the channel from the transmitter to the legitimate receiver, is known at the encoder non-causally but the state of the wiretapper's

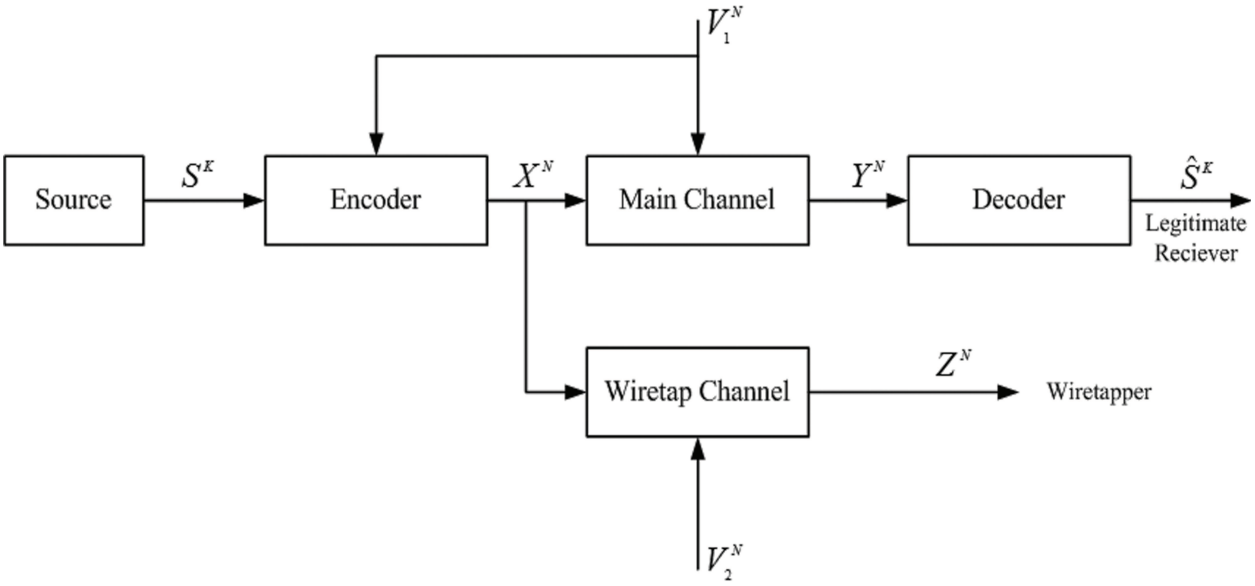

Fig. 4. The new more general wiretap channel with side information. The wiretapper's messages is not a degraded version of the legitimate receiver's one and the receiver and the wiretapper listen to the sent message from the separated channels with different channel states.

channel is unknown and the channels' states, i.e. V_{ti}, $t = 1, 2$, $1 \leq i \leq N$, are independent and identically distributed (i.i.d), but V_{1i} and V_{2i} are correlated. The transmitter sends the message $s^k \in \{1, 2, \ldots, M\}$ to the legitimate receiver in N channel uses. Based on the s^k and v^N, the encoder generates the codeword x^N and transmits it on the main and the wiretap channels. The decoder at the legitimate receiver makes an estimation of the transmitted message $\hat{s}^k$ based on the received message y^N. The corresponding output at the wiretapper is z^N. The channels are memoryless, i.e.,

$$p(y^N|x^N, v^N) = \prod_{i=1}^{N} p(y_i|x_i, v_i) \tag{1}$$

$$p(z^N|x^N, v^N) = \prod_{i=1}^{N} p(z_i|x_i, v_i) \tag{2}$$

Assume that S^k is uniformly distributed on $\{1, 2, \ldots, M\}$, so $H(S^k) = \log M$. The average probability of error P_e is given by

$$P_e = \frac{1}{M} \sum_{i=1}^{M} Pr(\hat{S}^k(Y^N) \neq i | S^k = i) \tag{3}$$

We define the rate of the transmission to the intended receiver to be

$$R = \frac{\log M}{N} \tag{4}$$

and the fractional equivocation wiretapper to be

$$d = \frac{H(S^k|Z^N)}{H(S^k)} \tag{5}$$

Obviously, we have $H(S^k|Z^N) = NRd$.

III. MAIN RESULTS:

OUTER AND INNER BOUNDS

Like [8], we say that the pair (R^*, d^*) is achievable, if for all $\epsilon > 0$, there exists an encoder-decoder pair such that

$$R \geq R^* - \epsilon, d \geq d^* - \epsilon, P_e \leq \epsilon. \tag{6}$$

Definition 1: The *secrecy capacity* C_s is the maximum R^* such that $(R^*, 1)$ is achievable.

Definition 2: We denote

$$R_{U1} = I(U;Y) - \max\{I(U;V_1,V_2), I(U;Z)\} \tag{7}$$

$$R_{U2} = I(U;Y) - I(U;V_1,V_2) \tag{8}$$

$$d_{U2} = \frac{R_{U1}}{R_{U2}} = \frac{I(U;Y) - \max\{I(U;V_1,V_2), I(U;Z)\}}{I(U;Y) - I(U;V_1,V_2)} \tag{9}$$

where U is an auxiliary random variable such that $U \rightarrow (X, V_1, V_2) \rightarrow (Y, Z)$ forms a Markov chain. Now, consider the following result:

Theorem 1: For the discrete memoryless channel with side information shown in Fig. 4, we denote $\mathcal{R}_U$ as the set of points (R, d) with $R_{U1} \leq R \leq R_{U2}$, $0 \leq d \leq 1$ and $Rd = R_{U1}$. Let

$$\mathcal{R}_U^{'} \triangleq \{(R^{'}, d^{'}) : 0 \leq R^{'} \leq R, 0 \leq d^{'} \leq d, (R, d) \in \mathcal{R}_U\}. \tag{10}$$

Then the set $\mathcal{R}$, defined as following, is achievable:

$$\mathcal{R} = \bigcup_{U \rightarrow (X,V_1,V_2) \rightarrow (Y,Z)} \mathcal{R}_U^{'}. \tag{11}$$

The region is achievable if we limit the cardinality of U by the constraint $|\mathcal{U}| \leq |\mathcal{X}||\mathcal{V}_1||\mathcal{V}_2| + 4$.

Proof: The proof of the theorem is relegated to the next Section. The constraint is implied by lemma 3 of [16]. ■

Remark 1: The point (R, d) in $\mathcal{R}$ with $d = 1$ is of considerable interest. These situations correspond to the perfect secrecy situation, defined as

$$R_s = \max_{U \to (X,V_1,V_2) \to (Y,Z)} R_{U1} \tag{12}$$

The following theorem bounds the secrecy capacity of the proposed wiretap channel with the side information.

Theorem 2: For the discrete memoryless wiretap channel with side information, shown in Fig. 4, we have

$$R_s \leq C_s \leq \min\{C_M, \max_{U \to (X,V_1,V_2) \to (Y,Z)} [I(U;Y) - I(U;Z)]\} \tag{13}$$

where C_M is the capacity of the main channel.

Proof: From Theorem 1, we have $R_s \leq C_s \leq C_M$ and from the result by Csiszár and Körner [3] we have $C_s \leq \max_{U \to (X,V_1,V_2) \to (Y,Z)} [I(U;Y) - I(U;Z)]$. This completes the proof. ■

IV. The Proof of Theorem 1

In this Section, we prove the achievability of the region $\mathcal{R}$. We prove that the rate equivocation pairs $(R_{U1}, 1)$ and (R_{U2}, d_{U2}) are achievable and then by implying time–sharing, achievability of the region $\mathcal{R}_U^{'}$ is proved.

A. $(R_{U1}$, 1) is Achievable

First we construct random codebooks by the following generation steps:

1) Codebook Generation: .

a. Generate $2^{N[I(U;Y)-\epsilon_{UY}]}$ i.i.d sequences u^N, according to the distribution $p(u^N) = \prod_{i=1}^{N} p(u_i)$.

b. Partition these u^N sequences into 2^{NR} bins where $R = [R_{U1} - \epsilon_{UY} - \epsilon_{UV_1V_2Z}]$. Index each bin by $j \in \{1, 2, \ldots, 2^{NR}\}$. Thus each bin contains $2^{N[max\{I(U;V_1,V_2),I(U;Z)\}+\epsilon_{UV_1V_2Z}]}$ sequences.

c. Distribute $2^{N[max\{I(U;V_1,V_2),I(U;Z)\}+\epsilon_{UV_1V_2Z}]}$ sequences randomly into $2^{N[max\{I(U;V_1,V_2),I(U;Z)\}-I(U;Z)+\epsilon_{UV_1V_2Z}+\epsilon_{UZ}]}$ subbin such that every subbin contains $2^{N[I(U;Z)-\epsilon_{UZ}]}$ sequences. Then index each subbin which contains U^N by

$$w \in \{1, 2, \ldots 2^{N[max\{I(U;V_1,V_2),I(U;Z)\}-I(U;Z)+\epsilon_{UV_1V_2Z}+\epsilon_{UZ}]}\}.$$

2) Encoding: To transmit message j thorough the main channel with interference v_1^N, the transmitter finds j-th bin of the sequence $u^N(j)$ such that $(u^N, v_1^N) \in T_\epsilon^N(P_{UV_1})$. We use $T_\epsilon^N(P_{UV_1})$ to denote the strong typical set based on the distribution P_{UV_1}, otherwise choose $j = 1$. The transmitter sends the associated jointly typical $x^N(j)$ generated according to $p(x^N(j)|u^N(j), v_1^N) = \prod_{i=1}^N p(x_i|u_i, v_{1,i})$

3) Decoding: The intended receiver receives y^n according to the distribution $\prod_{i=1}^N p(y_i|x_i, v_{1,i})$. Then it looks for the unique sequence u^N such that $(u^N, v_1^N) \in T_\epsilon^N(P_{UV_1})$ and the index of the bin containing u^N is declared as the transmitted message.

4) Wiretapper: The wiretapper receives a sequence z^N according to $\prod_{i=1}^N p(z_i|x_i, v_{2,i})$.

Now, we prove that $(R_{U1}, 1)$ is achievable. As the first step we should prove that $P_e \longrightarrow 0$, as $N \to \infty$. Our encoding-decoding strategy is similar to the one used in [8] and it is easy to show that the information rate R_{U1} in the main channel is achievable. For more detail see Appendix A in [8]. As the second step, we should prove that $d \to 1$, as $N \to \infty$. In this step, we consider the uncertainty of the message to the wiretapper. So we have

$$
\begin{aligned}
&H(S^k|Z^N) \\
&\quad = H(S^k, Z^N) - H(Z^N) \\
&\quad = H(S^k, Z^N, W) - H(W|S^k, Z^N) - H(Z^N) \\
&\quad = H(S^k, Z^N, W, U^N) - H(U^N|S^k, Z^N, W) - H(W|S^k, Z^N) - H(Z^N) \\
&\quad = H(S^k, W|Z^N, U^N) + H(U^N, Z^N) - H(U^N|S^k, Z^N, W) - H(W|S^k, Z^N) - H(Z^N) \\
&\quad \geq^{(a)} H(U^N|Z^N) - H(U^N|S^k, Z^N, W) - H(W|S^k, Z^N) \\
&\quad \geq^{(b)} H(U^N|Z^N) - H(U^N|S^k, Z^N, W) - \log|\mathcal{W}| - H(U^N|Y^N) \\
&\quad =^{(c)} N[I(U;Y) - I(U;Z)] - H(U^N|S^k, Z^N, W) \\
&\quad -N[max\{I(U;V_1,V_2), I(U;Z)\} - I(U;Z) + \epsilon_{UV_1V_2Z} + \epsilon_{UZ}] \\
&\quad = NR_{U1} - H(U^N|S^k, Z^N, W) - N[\epsilon_{UV_1V_2Z} + \epsilon_{UZ}]
\end{aligned}
\tag{14}
$$

where

(a) follows from the fact that $H(S^k, W|Z^N, U^N) \geq 0$;

(b) is because of the fact that $H(W|S^k, Z^N) \leq H(W) \leq \log|\mathcal{W}|$ and $H(U^N|Y^N) \geq 0$;

(c) follows from the fact that $I(U^N; Y^N) = NI(U; Y)$, $I(U^N; Z^N) = NI(U; Z)$ and

$$log|\mathcal{W}| = N[max\{I(U; V_1, V_2), I(U; Z)\} - I(U; Z) + \epsilon_{UV_1V_2Z} + \epsilon_{UZ}].$$

To compute the second term in (14), we should bound the entropy of the codeword conditioned on the bin j, subbin w and the wiretapper's received signal z^N. We consider the subbin w in bin j as a codebook, U^N in the codebook as the input message and Z^N as the result of passing U^N through the wiretap channel. From Z^N, the decoder estimates the sent message U^N. Let $g(\cdot)$ be the decoder and the estimate be $\hat{U}^N = g(\cdot)$. Define the probability of error

$$P_{SB} = Pr\{\hat{U}^N \neq U^N\}. \tag{15}$$

By Fano's inequality [17], we have

$$H(U^N|S^k = j, W = w, Z^N) \leq h(P_{SB}) + P_{SB}N[I(U; Z) - \epsilon_{UZ}]. \tag{16}$$

Hence

$$H(U^N|S^k, W, Z^N) \leq h(P_{SB}) + P_{SB}N[I(U; Z) - \epsilon_{UZ}]. \tag{17}$$

Now, we should prove that for arbitrary $0 < \lambda < 1/2$, $P_{SB} \leq \lambda$. The proof is similar to the one in [8]. Thus, we have bounded P_{SB} for given arbitrary small ϵ and λ.

Combining (5), (14), (17) and the bound on P_{SB} we have

$$d \geq 1 - \frac{\epsilon_{UZ} - \epsilon_{UY} - h(\lambda)/N + \lambda[I(U; Z) - \epsilon_{UZ}]}{R_{U1} - \epsilon_{UY} - \epsilon_{UV_1V_2Z}}. \tag{18}$$

Thus we derive that $d \to 1$, as $N \to \infty$.

B. (R_{U2}, d_{U2}) *is Achievable*

From the (7)- (9), it is derived that if $I(U;V_1,V_2) \geq I(U;Z)$, then the equivocation rate pair (R_{U2}, d_{U2}) is equal with $(R_{U1}, 1)$. So, we should prove that if $I(U;V_1,V_2) < I(U;Z)$, then (R_{U2}, d_{U2}) is achievable. In this case, when $I(U;V_1,V_2) < I(U;Z)$, we have

$$R_{U2} = I(U;Y) - I(U;V_1,V_2) \tag{19}$$

$$d_{U2} = \frac{I(U;Y)-I(U;Z)}{I(U;Y)-I(U;V_1,V_2)} \tag{20}$$

Now we introduce the encoding and decoding strategy.

1) Codebook Generation: .

a. Generate $2^{N[I(U;Y)-\epsilon_{UY}]}$ i.i.d sequences u^N, according to the distribution $p(u^N) = \prod_{i=1}^{N} p(u^N)$.

b. Partition these sequences into 2^{NR} bins where $R = [R_{U2} - \epsilon_{UY} - \epsilon_{UV_1V_2}]$. Index each bin by $j \in \{1, 2, \ldots, 2^{NR}\}$. Thus each bin contains $2^{N[I(U;V_1,V_2)+\epsilon_{UV_1V_2Z}]}$ sequences.

c. Distribute $2^{N[max\{I(U;V_1,V_2),I(U;Z)\}+\epsilon_{UV_1V_2Z}]}$ sequences randomly into $2^{N[max\{I(U;V_1,V_2),I(U;Z)\}-I(U;Z)+\epsilon_{UV_1V_2Z}+\epsilon_{UZ}]}$ subbins such that every subbin contains $2^{N[I(U;Z)-\epsilon_{UZ}]}$ sequences. Then index each subbin containing U^N by $w \in \{1, 2, \ldots 2^{N[max\{I(U;V_1,V_2),I(U;Z)\}-I(U;Z)+\epsilon_{UV_1V_2Z}+\epsilon_{UZ}]}\}$.

2) Encoding: To transmit message j thorough the main channel with interference v_1^N, transmitter finds bin j for a sequence $u^N(j)$ such that $(u^N, v_1^N) \in T_\epsilon^N(P_{UV_1})$, otherwise choose $j = 1$.

3) Decoding: The intended receiver receives y^n according to the distribution $\prod_{i=1}^{N} p(y_i|x_i, v_{1,i})$. Then the receiver looks for the unique sequence u^N such that $(x^N, v_1^N) \in T_\epsilon^N(P_{UV_1})$ and the index bin of the bin containing u^N declares as the message index.

4) Wiretapper: The wiretapper receives a sequence z^N according to $\prod_{i=1}^{N} p(z_i|x_i, v_{2,i})$.

To prove that (R_{U2}, d_{U2}) is achievable, first we should prove that $P_e \to 0$, as $N \to \infty$. The proof is similar to the one in Section IV-A. Then we should prove that $d_{U2} \to \frac{I(U;Y)-I(U;Z)}{I(U;Y)-I(U;V_1,V_2)}$, as $N \to \infty$. For this purpose we

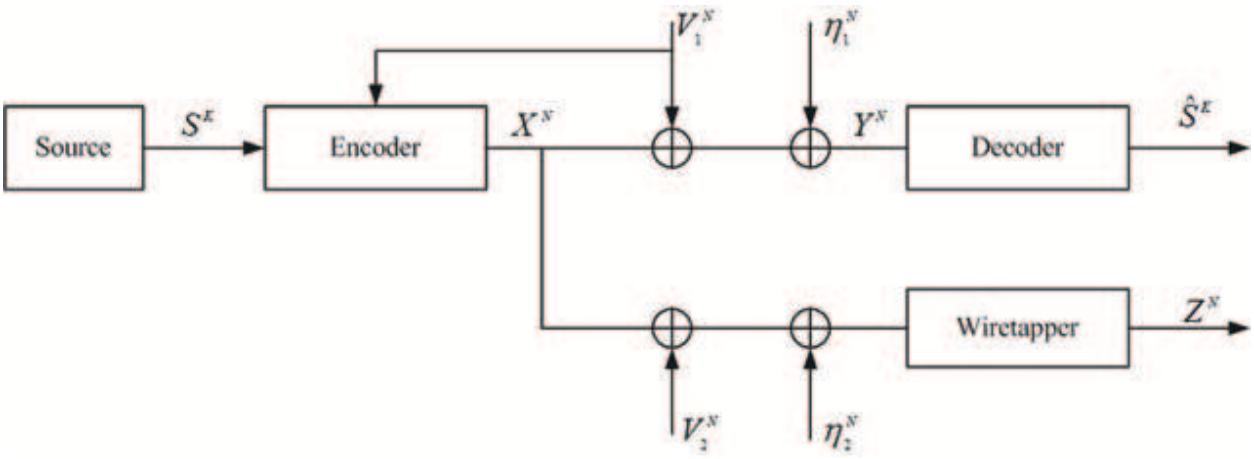

Fig. 5. The new more general Gaussian wiretap channel with side information. The receiver and the wiretapper listen to the sent message from the separated channels with channel states. These channel states may have some correlation to each other.

can follow the strategy in Section IV-A. So we have

$$\begin{aligned} & H(S^k|Z^N) \\ & \geq N[I(U;Y) - I(U;Z)] - H(U^N|S^k, Z^N) \end{aligned} \tag{21}$$

and for the second term in (21) like (15) – (17) we have

$$H(U^N|S^k, W, Z^N) \leq h(P_{SB}) + P_{SB}N[I(U;Z) - \epsilon_{UZ}]. \tag{22}$$

So, combining the above results, we have

$$d \geq \frac{R_{U2}}{R_{U2} - \epsilon_{UY} - \epsilon_{UV_1V_2}} d_{U2} - \frac{h(\lambda)/N + \lambda[I(U;V_1,V_2)] + \epsilon_{UV_1V_2}}{R_{U2} - \epsilon_{UY} - \epsilon_{UV_1V_2}}. \tag{23}$$

Thus we have $d_{U2} \to \frac{I(U;Y)-I(U;Z)}{I(U;Y)-I(U;V_1,V_2)}$, as $N \to \infty$.

V. A New Gaussian Wiretap Channel

In this Section we extend Theorem 1 to the Gaussian case like the approach taken in [8], using the same auxiliary random variable U. For the new Gaussian wiretap channel shown in Fig. 5, we have the following results based on Theorem 1.

Theorem 3: (Theorem 1 in Gaussian case For the Gaussian wiretap channel shown in Fig. 5) Using the auxiliary random variable $U = X + \alpha V_1$, where α is a real number and ρ_{XV_1} is the correlation coefficient of X and V_1, we

denote $\mathcal{R}_U$ as the set of points (R, d) with $R_{U1} \leq R \leq R_{U2}$, $0 \leq d \leq 1$, $Rd = R_{U1}$, where R_{U1} and R_{U2} are defined in (7) and (8). By defining

$$\mathcal{R}_U^{'} \triangleq \{(R^{'}, d^{'}) : 0 \leq R^{'} \leq R, 0 \leq d^{'} \leq d, (R, d) \in \mathcal{R}_U\}, \tag{24}$$

the set $\mathcal{R}$, defined as follows, is achievable:

$$\mathcal{R} = \bigcup_{U=X+\alpha V_1, \alpha \in \mathbb{R}} \mathcal{R}_U^{'}. \tag{25}$$

Proof: The proof is similar to the proof of Theorem 1. We only need to show that $\mathcal{R}_U$ is achievable for the specified α and U. Assuming transmitter has the power constraint P, the side information in the main channel satisfies $V_1 \sim \mathcal{N}(0, Q_1)$, the wiretap channel has the side information, satisfying $V_2 \sim \mathcal{N}(0, Q_2)$, ρ_{XV_1}, ρ_{XV_2} and $\rho_{V_1V_2}$ represent the correlation coefficient between X, V_1 and V_2 and $P^{'} = P[1 + 4\epsilon \ln 2 + \frac{\rho_{XV_1}^2}{1-\rho_{XV_1}^2}]^{-1}$ (see Appendix A), we use some modification in the proof of $\mathcal{R}_{U1}$ as follows.

In the codebook generation, sequence u^N are generated according to $f(u^N) = \prod_{i=1}^{N} f(u_i)$, where $f(u_i) \sim \mathcal{N}(0, P^{'} + \alpha^2 Q_1)$ for all $i \in \{1, 2, \ldots, N\}$. In the encoding process, $x^N(j) = u^N(j) - \alpha v_1^N$. The intended receiver observes $y^N = x^N + v_1^N + \eta_1^N$ and the wiretapper observes $z^N = x^N + v_2^N + \eta_2^N$. As a source constraint, we should introduce potential error $E^X(j)$, which represents in the encoding process and $x^N(j) = u^N(j) - \alpha v_1^N$ does not satisfy the power constraint.

Then, provided that there is at least one sequence $u^N(j)$ jointly typical with v_1^N, the probability of error $E^X(j)$ tends to zero. Therefore, the modifications do not influence the achievability proof of $\mathcal{R}_U$. Assuming ϵ is arbitrarily small, since $P^{'} \to P$. ■

Now, we calculate $I(U;Y)$, $I(U;V_1,V_2)$ and $I(U,Z)$, with respect to $U = X + \alpha V_1$. We have

$$I(U;Y)$$

$$= \tfrac{1}{2}\log[\tfrac{(P+\alpha^2Q_1+2\alpha\rho_{XV_1}\sqrt{PQ_1})(P+Q_1+N_1+2\rho_{XV_1}\sqrt{PQ_1})}{(P+\alpha^2Q_1+2\alpha\rho_{XV_1}\sqrt{PQ_1})(P+Q_1+N_1+2\rho_{XV_1}\sqrt{PQ_1})-(P+\alpha Q_1+(\alpha+1)\rho_{XV_1}\sqrt{PQ_1})^2}] \tag{26}$$

$$I(U;V_1,V_2) = \tfrac{1}{2}\log[\tfrac{(1-\rho^2_{V_1V_2})(P+\alpha^2Q_1+2\alpha\rho_{XV_1}\sqrt{PQ_1})}{P(1-\rho^2_{XV_1}-\rho^2_{XV_2}-\rho^2_{V_1V_2}+2\rho_{XV_1}\rho_{XV_2}\rho_{V_1V_2})}] \tag{27}$$

$$I(U;Z)$$

$$= \tfrac{1}{2}\log[\tfrac{(P+\alpha^2Q_1+2\alpha\rho_{XV_1}\sqrt{PQ_1})(P+Q_2+N_2+2\rho_{XV_2}\sqrt{PQ_2})}{(P+\alpha^2Q_1+2\alpha\rho_{XV_1}\sqrt{PQ_1})(P+Q_2+N_2+2\rho_{XV_2}\sqrt{PQ_2})-(P+\rho_{XV_2}\sqrt{PQ_2}+\alpha\rho_{XV_1}\sqrt{PQ_1}+\alpha\rho_{V_1V_2}\sqrt{Q_1Q_2})^2}] \tag{28}$$

Then, we introduce *Leakage Function* $\Delta I(\alpha)$ which is defined as $\Delta I(\alpha) = I(U;Z) - I(U;V_1V_2)$. Thus, we have

$$\Delta I(\alpha) = I(U;Z) - I(U;V_1V_2)$$

$$= \tfrac{1}{2}\log[\tfrac{P(P+Q_2+N_2+2\rho_{XV_2}\sqrt{PQ_2})(1-\rho^2_{XV_1}-\rho^2_{XV_2}-\rho^2_{V_1V_2}+2\rho_{XV_1}\rho_{XV_2}\rho_{V_1V_2})}{(P+\alpha^2Q_1+2\alpha\rho_{XV_1}\sqrt{PQ_1})(P+Q_2+N_2+2\rho_{XV_2}\sqrt{PQ_2})-(P+\rho_{XV_2}\sqrt{PQ_2}+\alpha\rho_{XV_1}\sqrt{PQ_1}+\alpha\rho_{V_1V_2}\sqrt{Q_1Q_2})^2}] \tag{29}$$

Hence

$$\Delta I(0) = \frac{1}{2}\log[\frac{(P+Q_2+N_2+2\rho_{XV_2}\sqrt{PQ_2})(1-\rho^2_{XV_1}-\rho^2_{XV_2}-\rho^2_{V_1V_2}+2\rho_{XV_1}\rho_{XV_2}\rho_{V_1V_2})}{Q_2(1-\rho^2_{XV_2})+N_2+2\rho_{XV_2}\sqrt{PQ_2}}] > 0 \tag{30}$$

and we can find two points α_0 and α_{-0} in which

$$\Delta I(\alpha_0) = \Delta I(\alpha_{-0}) = 0. \tag{31}$$

Furthermore, there is a point α^* in which $\Delta I(\alpha)$ is maximized, i.e.,

$$\alpha^* = -\frac{(\rho_{XV_1}\sqrt{PQ_1}+\rho_{V_1V_2}\sqrt{Q_1Q_2})(P+\rho_{XV_2}\sqrt{PQ_1})-\rho_{XV_1}\sqrt{PQ_1}(P+N_2+Q_2+2\rho_{XV_2}\sqrt{PQ_2})}{(\rho_{XV_1}\sqrt{PQ_1}+\rho_{V_1V_2}\sqrt{Q_1Q_2})^2-2Q_1(P+N_2+Q_2+2\rho_{XV_2}\sqrt{PQ_2})} \tag{32}$$

where

$$\max\Delta I(\alpha) = \Delta I(\alpha^*) \tag{33}$$

Now, we want to study the leakage function. So, denote $R(\alpha) = I(U;Y) - I(U;V_1,V_2)$ and $R_Z(\alpha) = I(U;Y) - I(U;Z)$. Because of the complexity of the results, we consider two special cases.

A. Case I

As the first condition, we assume that $Q_1 = Q_2 = Q$, $\rho_{XV_1} = \rho_{XV_2} = 0$ and $\rho_{V_1V_2} = 1$. In this case our model reduces to the channel introduced [8] and we have

$$R(\alpha) = \frac{1}{2}\log[\frac{P(P+Q+N_1)}{(P+\alpha^2 Q)(P+Q+N_1)-(P+\alpha Q)^2}] \tag{34}$$

which is maximized by $\alpha^* = \frac{P}{P+N}$ as described in [7] and achieves $C_M = \frac{1}{2}\log[\frac{P+N}{N}]$, in which C_M is the maximum rate of the main channel. It can be found easily that $R(\alpha)$ is an increasing function with respect to α as $\alpha < \alpha^*$, a decreasing function with respect to α as $\alpha > \alpha^*$.

Similarly, the rate R_Z has two extremum points in $\alpha = 1$ and $\alpha = -\frac{P}{Q}$ and it can be shown that R_Z is a decreasing function with respect to α as $\alpha < -\frac{P}{Q}$ or $1 < \alpha$ and an increasing function with respect to α as $-\frac{P}{Q} < \alpha < 1$. Then we state the following result.

Theorem 4: For the new Gaussian wiretap channel with side information illustrated in Fig. 5, under the special conditions explained in Case I, rate equivocation pair (R, d) is achievable if

$$\begin{aligned} &R \le C_M \\ &d \le 1 \\ &Rd \le \begin{cases} C_M & 0 < P \le P_1 \\ \begin{cases} R(\alpha_0) & R \le R(\alpha_0) \\ R_Z(\alpha) & R(\alpha_0) \le R \le C_M \end{cases} & P_1 \le P \le P_2 \\ \begin{cases} R_Z(1) & R \le R(1) \\ R_Z(\alpha) & R(1) \le R \le C_M \end{cases} & P_2 \le P \end{cases} \end{aligned} \tag{35}$$

where

$$P_1 = -N_1 - \frac{Q}{2} + \frac{\sqrt{Q^2+4QN_2}}{2} \tag{36}$$

$$P_2 = -\frac{Q}{2} + \frac{\sqrt{Q^2+4Q(N_1+N_2)}}{2} \tag{37}$$

We should note that this rate equivocation pair is similar the one presented in [8] and the proof can be found there. It is clear that under the assumed conditions, our channel reduces to the previous model [8] and we obtain similar result.

Corollary 1: [8, Theorem 4-5] For the proposed Gaussian wiretap channel with side information in Case I, the side information helps to achieve larger rate equivocation region. The proof is similar to the one in [8].

B. Case II

As the second special case, we assume that $Q_1 = Q_2 = Q$, $\rho_{XV_1} = \rho_{XV_2} = \rho_{V_1V_2} = 0$ and $N_1 \neq N_2$. In this case we have

$$R(\alpha) = \frac{1}{2}\log[\frac{P(P+Q+N_1)}{(P+\alpha^2 Q)(P+Q+N_1)-(P+\alpha Q)^2}] \tag{38}$$

which is maximized by $\alpha^* = \frac{P}{P+N}$ and achieves C_M. It can be found that the rate R_Z has two extremum points in $\alpha = 1$ and $\alpha = -\frac{P}{Q}$. As we can see, this points are similar to the one for the functions in the previous case. So, we state the following result for this case.

Theorem 5: For the proposed Gaussian wiretap channel with side information in Fig. 5, under the special conditions, a rate pair (R, d) is achievable if

$$\begin{aligned} &R \leq C_M \\ &d \leq 1 \\ &Rd \leq \begin{cases} C_M & 0 < P \leq P_3 \\ \begin{cases} R(\alpha_0) & R \leq R(\alpha_0) \\ R_Z(\alpha) & R(\alpha_0) \leq R \leq C_M \end{cases} & P_3 \leq P \leq P_4 \\ \begin{cases} R_Z(1) & R \leq R(1) \\ R_Z(\alpha) & R(1) \leq R \leq C_M \end{cases} & P_4 \leq P \end{cases} \end{aligned} \tag{39}$$

where

$$P_3 = \frac{(Q-2N_1)+\sqrt{5Q^2+4Q(N_2-N_1)}}{2} \tag{40}$$

$$P_4 = \frac{Q}{2}+\frac{\sqrt{5Q^2+4QN_2}}{2} \tag{41}$$

So the obtained results are similar to the previous case for Gaussian wiretap channel with side information.

CONCLUSION

In this paper, a new applicable wiretap channel with side information was introduced. In this channel, the previous models were generalized. An achievable equivocation rate region for this channel was derived and then, our result were extended to the Gaussian case.

REFERENCES

[1] C.E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, pp. 656–715, October 1949.

[2] A. Wyner, "The wire-tap channel," *Bell. Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

[3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. on Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[4] C. Shannon, "Channels with side information at the transmitter," *J. Res. Devel.*, vol. 2, pp. 289–293, 1958.

[5] S. I. Ge'lfand and M. S. Pinsker, "Coding for channel with random parameters," *Probl. Inf. Theory*, vol. 9, no. 1, pp. 19–31, 1980.

[6] M. H. M. Costa, "Writing on dirty paper," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 3, pp. 439–441, May 1983.

[7] C. Mitrpant, H. Vinck, and Y. Luo, "An achievable region for the gaussian wiretap channel with side information," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2181–2190, 2006.

[8] Y. Chen and H. Vinck, "Wiretap channel with side information," *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 395–402, 2008.

[9] W. Liu and B. Chen, "Wiretap channel with two-sided channel state information," in *in Proc. 41st Asilomar Conf. Signals, Systems and Comp., Pacific Grove, CA,*, Nov. 2007, pp. 893–897.

[10] A. El Gamal, O. O. Koyluoglu, M. Youssef, and H. El Gamal, "The two way wiretap channel: Theory and practice," *available on: arXiv:1006.0778v1 [cs.IT]*, 4 Jun 2010.

[11] M. R. D. Rodrigues, A. Somekh-Baruch, and M. Bloch, "On gaussian wiretap channel with m-pam inputes," *European Wireless Conference*, pp. 774–781, 2010.

[12] E. Ekrem and S. Ulukus, "The secrecy capacity region of the gaussian mimo multi-receiver wiretap channel," *available on: arXiv:0903.3096v1 [cs.IT]*, 18 Mar 2009.

[13] A. Khisti, S. Diggavi, and G. Wornell, "Secret-key agreement with channel state information at the transmitter," *available on: arXiv:1009.3052v2 [cs.IT]*, 17 Sep 2010.

[14] A. Khisti, S. N. Diggavi, and G. W. Wornell, "Secret key agreement using asymmetry in channel state knowledge," *in Proc. IEEE International Symposium on Information Theory (ISIT), Seoul, South Korea*, pp. 2286–2290, July 2009.

[15] Y. Chia and A. El Gamal, "Wiretap channel with causal state information," 13 Jan 2010, Available from: http://arXiv:1001.2327v1 [cs.IT].

[16] R. Ahslwede and J. Korner, "Source coding with side information and a converse for degraded broadcast channe," *IEEE Trans. Inf. Theory*, vol. IT-21, no. 6, pp. 629–637, 1975.

[17] T. M. Cover and J. A. Thomas, *Elements of Onformation Theory*, John Wiley and Sons, Inc., 2006.

APPENDIX A

THE CONDITION ON AVERAGE POWER CONSTRAINT

In this Section we apply the following lemma to the condition on the average power constraint by letting $P^{'} = P[1+4\epsilon\ln 2+\frac{\rho^2_{XV_1}}{1-\rho^2_{XV_1}}]^{-1}$.

Lemma 1: Assume that X^N and V_1^N are two sequences of i.i.d random variables $X \sim \mathcal{N}(0,\sigma_X)$ and $V_1 \sim \mathcal{N}(0,\sigma_{V_1})$, respectively, with correlation coefficient ρ_{XV_1}. Let $U^N = X^N + \alpha V_1^N$, where α is a constant real number. If $(u^N,v^N) \in T^N_{U,V_1}(\epsilon)$, for any $\epsilon > 0$, and $\sigma_X \leq P[1+4\epsilon\ln 2+\frac{\rho^2_{XV_1}}{1-\rho^2_{XV_1}}]^{-1}$, then $[\sum_{i=1}^N x_i^2]/N \leq P$.

Proof: Since X^N and V_1^N are two sequences of i.i.d Gaussian random variables then $U^N \sim \mathcal{N}(0,\sigma_X + \alpha^2\sigma_{V_1} + 2\alpha\sigma_X\sigma_{V_1})$. Furthermore $(u^N,v^N) \in T^N_{U,V_1}(\epsilon)$ implies that

$$
\begin{aligned}
\epsilon > |-\frac{1}{N}\log p(u^N,v^N) - H(U,V)\,| \\
&= |-\tfrac{1}{N}\log p(u^N,v^N) - H(V) - H(U|V)| \\
&= |-\tfrac{1}{N}\log p(u^N,v^N) - H(V) - H(X|V)| \\
2\epsilon > |-\tfrac{1}{N}\log p(u^N,v^N) + \tfrac{1}{N}\log p(v^N) - H(X|V)| \\
&= |-\tfrac{1}{N}\log p(u^N|v^N) - H(X|V)| \\
&= |-\tfrac{1}{N}\log p(x^N|v^N) - H(X|V)| \\
&= |-\tfrac{1}{N}\textstyle\sum_{i=1}^N \log p(x_i|v_{1,i}) - H(X|V)| \\
&=^{(d)} \tfrac{1}{\ln 2}|\tfrac{1}{2N(1-\rho^2_{XV_1})}\textstyle\sum_{i=1}^N \frac{x_i^2}{\sigma_X^2} - 2\rho_{XV_1}\frac{x_iv_{1,i}}{\sigma_X\sigma_{V_1}} + \rho^2_{XV_1}\frac{v_{1i}^2}{\sigma_{V_1}^2} + \tfrac{1}{2}ln[2\pi\sigma_X^2(1-\rho^2_{XV_1})] - H(X|V)| \\
&=^{(e)} \tfrac{1}{\ln 2}|\tfrac{\sum_{i=1}^N x_i^2}{2N(1-\rho^2_{XV_1})\sigma_X^2} - \tfrac{\rho^2_{XV_1}}{2(1-\rho^2_{XV_1})} + \tfrac{1}{2}\ln[2\pi\sigma_X^2(1-\rho^2_{XV_1})] - \tfrac{1}{2}\ln[2\pi e\sigma_X^2(1-\rho^2_{XV_1})]| \\
&= \tfrac{1}{\ln 2}|\tfrac{\sum_{i=1}^N x_i^2}{2N(1-\rho^2_{XV_1})\sigma_X^2} - \tfrac{\rho^2_{XV_1}}{2(1-\rho^2_{XV_1})} - \tfrac{1}{2}|
\end{aligned}
\tag{42}
$$

where (d) is because of the jointly distribution function of $(x_i, v_{1,i})$ and (e) is because that

$$H(X|V) = H(X) - I(X;V_1) = \frac{1}{2}\ln(2\pi e\sigma_X^2) - \frac{1}{2}\ln(\frac{\sigma_X^2\sigma_{V_1}^2}{\sigma_X^2\sigma_{V_1}^2 - \sigma_{XV_1}^2})$$
$$= \tfrac{1}{2}\ln[2\pi e\sigma_X^2(1-\sigma_{XV_1}^2)] \tag{43}$$

Thus

$$\frac{1}{N}\sum_{i=1}^{N} x_i^2 < \sigma_X^2[4\epsilon\ln 2 + \frac{\rho_{XV_1}^2}{1-\rho_{XV_1}^2} + 1] \tag{44}$$

and with the condition on the average power constraint $\sigma_X \leq P[1+4\epsilon\ln 2+\frac{\rho_{XV_1}^2}{1-\rho_{XV_1}^2}]^{-1}$, we have $[\sum_{i=1}^{N} x_i^2]/N \leq P$.

■